Department of Mental Health & Substance Abuse Services

Policies and Procedures

Subject: Notification in Case of Breach

Policy Number: HIPAA 3.5

Effective Date: 1/11/18

Entity Responsible: Office of General Counsel

Revision Date:

1. Purpose:

To provide procedures to the Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) on how to notify each individual whose unsecured protected health information (PHI) has been, or is reasonably believed by TDMHSAs or the RMHIs to have been accessed, acquired, used, or disclosed as a result of a breach.

2. Policy:

2.1: The TDMHSAS and the RMHIs will notify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of a breach.

2.2: A breach excludes the following:

2.2.1: any unintentional acquisition, access, or use of PHI by a member of the TDMHSAS or the RMHI or person acting under the authority of TDMHSAS or the RMHI or a Business Associate of TDMHSAS or the RMHI, if made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the HIPAA privacy rules and regulations; or

2.2.2: any inadvertent disclosure by a person who is authorized to access PHI at TDMHSAS or the RMHIs or a Business Associate of TDMHSAS or the RMHIs to another person who also authorized to access the PHI at TDMHSAS or the RMHIs or a Business Associate, and the information

received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA privacy rules and regulations; or

2.2.3: a disclosure of PHI where TDMHSAS, the RMHIs, or a Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.3: An acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy rules and regulations is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based upon a risk assessment which includes the following factors:

2.3.1: the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2.3.2: the unauthorized person who used the PHI or to whom the disclosure was made;

2.3.3: whether the PHI was actually acquired or viewed; and

2.3.4: the extent to which the risk to the PHI has been mitigated.

2.4: A breach is deemed to have been discovered by TDMHSAS or the RMHI as of the first day on which such breach is known to TDMHSAS or the RMHI, or, by exercising reasonable diligence would have been known to TDMHSAS or the RMHI.

2.5: TDMHSAs or the RMHI will be deemed to have knowledge of the breach if such breach is known, or by exercising reasonable diligence would have been known, to any person other than the person committing the breach, who is a workforce member of TDMHSAS or the RMHI.

3. Procedures/ Responsibilities:

3.1: Any member of the RMHI workforce who discovers a breach must immediately, upon discovery of such breach, notify their supervisor, RMHI Privacy Officer, and the RMHI Security Officer if such breach relates to the RMHIs. If the RMHI Privacy Officer and the RMHI Security Officer receives notification of a breach, they must immediately notify the TDMHSAS Privacy Officer and the TDMHSAS Security Officer. The TDMHSAS Privacy Officer and TDMHSAS Security Officer will then notify appropriate individuals within Central Office.

3.2: Any member of the TDMHSAS workforce who discovers a breach must immediately, upon discovery of the breach, notify their supervisor, the

TDMHSAS Privacy Officer, and the TDMHSAS Security Officer. The TDMHSAS Privacy Officer and the TDMHSAS Security Officer will then notify appropriate individuals within Central Office.

3.3: If the breach of unsecured PHI involves less than 500 residents of a State, TDMHSAS will provide notification to the individuals regarding the breach. Such notification without unreasonable delay and must be provided within sixty (60) calendar days of the discovery of the breach. The notification will be written in plain language and include:

3.3.1: a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

3.3.2: a description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3.3.3: any steps individuals should take to protect themselves from potential harm resulting from the breach;

3.3.4: a brief description of what TDMHSAS and/ or the RMHI is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

3.3.5: contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

3.4: If the breach of unsecured PHI involves less than 500 residents of a State, TDMHSAS will provide the notification described in 3.3 in the following form:

3.4.1: Written notification by first-class mail to the individual at the last known address of the individual, or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

3.4.1.2: If TDMHSAS or the RMHI knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification provided by first-class mail may be provided to either of those parties. If TDMHSAS or the RMHI is unable to provide notification to next of kin or personal representative due to insufficient or out-of-date contact

information, substitute notification (as described below) is not necessary.

3.4.2: If there is insufficient or out-of-date information that precludes the written notice described above, the TDMHSAS or the RMHI may provide a substitute form of notice as described below:

3.4.2.1: If a substitute form of notice is needed for fewer than ten (10) individuals, such substitute notice may be provided in alternative form of written notice, telephone, or other means; or

3.4.2.2. If substitute form notice is needed for more than ten (10) individuals, such substitute notice may be provided in a conspicuous posting for a period of ninety (90) days on the TDMHSAS and/or the RMHIs homepage of their Websites, or in major print or broadcast media in geographic areas where the individuals affected in the breach are likely to reside, and include a toll-free phone number that remains active for the ninety (90) day period where an individual can learn if their unsecured PHI was included in the breach.

3.4.3: If TDMHSAS and/or the RMHI determines the situation requires urgency because of possible imminent misuse of unsecured PHI, notice may be provided to individuals by telephone, or other means, as appropriate, in addition to the notification methods described above.

3.5: If the breach of unsecured PHI involves more than 500 residents of a State, TDMHSAS shall notify prominent media outlets service the State. This notification must be provided without unreasonable delay and within sixty (60) calendar days of the discovery of the breach. The notification will be written in plain language and include:

3.5.1: a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

3.5.2: a description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3.5.3: any steps individuals should take to protect themselves from potential harm resulting from the breach;

3.5.4: a brief description of what TDMHSAS and/ or the RMHI is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

3.5.5: contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

3.6: In the case of any breach of unsecured PHI, the TDMHSAS shall notify the Department of Health and Human Services (DHHS) in the manner specified on the DHHS website.

3.6.1: For breaches involving less than 500 individuals, the TDMHSAS Privacy Officer shall keep a log or other documentation, and not later than 60 days after the end of the calendar year, provide the notification described above.

3.6.2: For breaches involving more than 500 individuals, the TDMHSAS shall contemporaneously provide the notification described above with the notice required in 3.5.

3.7: Any Business Associate shall, following the discovery of a breach of unsecured PHI, notify the TDMHSAS without unreasonable delay and not later than sixty (60) days after discovery of the breach. The notification shall include:

3.7.1: the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired, used, or disclosed during the breach; and

3.7.2: any other available information, as it becomes available, that the TDMHSAS and the RMHI is required to provide in their notification to the individuals as described in 3.3 and 3.5.

3.8: If a law enforcement official states to TDMHSAS or the RMHI or a Business Associate of TDMHSAS or the RMHI, that a notification or posting described above and required under the law would impede a criminal investigation or cause damage to national security, the TDMHSAS, RMHI, or the Business Associate of the TDMHSAS or RMHI shall:

3.8.1: if the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

3.8.2: if the statement is made orally, the TDMHSAS Privacy Officer should document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no

longer than thirty (30) days from the date of the oral statement, unless a written statement as described above is provided during that time.

3.1: The supervisor of any TDMHSAS or RMHI workforce member found to have violated HIPAA or TDMHSAS HIPAA Policies and Procedures is responsible for recommending the appropriate level of discipline in accordance with TDMHSAS' personnel rules, policies, procedures, and guidelines.

3.2: All members of the TDMHSAS and RMHIs workforce must be trained on HIPAA, and TDMHSAS HIPAA Policies and Procedures. Members who violate the above mentioned laws, policies, and procedures after receiving such training may be warned (written or verbal), suspended, transferred, demoted, or terminated, depending on the nature or severity of the violation.

4. Other Considerations:

4.1: Authority

45 C.F.R §§ 164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.410, 164.412

Approved:

Marie Williams vg
Commissioner

1-11-18
Date